REMARKS

The non-final Office Action of March 7, 2007 has been carefully reviewed and these remarks are responsive thereto. Claims 1-2, 4-13, 15, 19-22, 24, 26-32, 34-38, and 45-54 have been canceled without prejudice or disclaimer, claim 55 has been amended, and new claims 61-81 have been added. Claims 55-81 remain pending in this application. Reconsideration and allowance of the instant application are respectfully requested.

Rejections Under 35 U.S.C. § 103

Claims 55-60 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,101,543 (Alden), in view of U.S. Patent No. 6,412,009 (Erickson). Applicants respectfully traverse this rejection for at least the following reasons.

Independent claim 55 recites transmitting encrypted information from a first computer to an intermediate server computer through a firewall, and then "transmitting the encrypted information from the intermediate server over the second return path," to a second computer. Alden discloses intermediate servers as part of a network tunnel, but does not teach or suggest the establishment of a return path or the transmission of data over a return path, as recited in claim 55. As discussed in the Amendment filed October 19, 2006, the data transmitted from Alden's intermediate tunnel servers to the tunnel endpoints is transmitted directly through the firewall. (Alden, col. 6, lines 24-67.) In other words, Alden does not transmit data over a "return path," as recited in claim 55. Rather, Alden transmits directly into the firewalls protecting the tunnel endpoints, thus requiring these firewalls to be "programmed to pass packets received over transport layer connection 2 into a private network on the other side of the firewall." (Alden, col. 6, lines 37-39.)

The Office Action alleges that transmitting encrypted information from an intermediate server over a return path to a recipient is disclosed by Alden at col. 8, lines 45-67. The relied-upon portion of Alden relates to transmitting a request frame and a response frame over a previously established transport layer connection, to communicate key encryption and authentication information between the tunnel endpoints. However, Alden's previously established transport layer connection involves transmitting data directly to the pre-programmed firewall, rather than establishing or transmitting via a return path. (Alden, col. 6, lines 24-67.)

Thus, Alden's request and response frames are not sent over a "return path," as recited in claim 55. Accordingly, Applicants submit that Alden does not teach or suggest, transmitting encrypted information from a first computer to an intermediate server computer through a firewall, and then "transmitting the encrypted information from the intermediate server over the second return path," as recited in claim 55.

Erickson also does not teach or suggest transmitting encrypted information from an intermediate server to a recipient computer over a return path, as recited in claim 55. Erickson thus fails to overcome the above-discussed deficiencies of Alden. Accordingly, Applicants submit that amended claim 55 not obvious over the proposed combination of Alden and Erickson.

Additionally, claim 55 respectively recites in steps (1) and (5) that the first and the second computer each transmit a request to establish a connection with the intermediate server computer. In contrast, Alden only describes techniques in which one endpoint computer of the network tunnel initiates communications via the tunnel servers, and the other endpoint computer is a passive recipient. (Alden, FIG. 3; col. 6, lines 24-67.) Similarly, Erickson describes a web client initiating communications to a web server via a tunneling mechanism. (Erickson, col. 3, lines 3-29) However, Erickson does not teach or suggest any configuration in which both endpoint computers initiate communications with an intermediate server. Thus, Applicants submit that claim 55 is allowable over the proposed combination of Alden and Erickson for this additional reason.

Independent claim 57 recites a method of communicating between a first computer protected by a first firewall and a second computer protected by a different second firewall, using a third intermediate computer situated between the two firewalls, in which an encrypted HTTP message from the first computer is received by the third computer and transmitted over a "receive channel" to the second computer. Since neither Alden nor Erickson teaches or suggests an intermediate computer transmitting an encrypted HTTP message over a receive channel, claim 57 is also not obvious over the proposed combination. Claims 56 and 58-60 each depend from claim 55 or 57, and are not obvious for at least the same reasons as their respective base claims, as well as based on the additional features recited therein.

For example, as discussed in the Amendment filed October 19, 2006, claim 56 recites, "in the intermediate server computer, decrypting encrypted information received from the first computer using encryption keys shared between the first computer and the intermediate

computer, and then re-encrypting the received information using encryption keys shared between the intermediate computer and the second computer." The Office Action alleges that Alden teaches this feature at col. 8, lines 45-67. However, the only encryption disclosed by Alden and similar tunneling systems takes place between the two endpoints of the tunnel connection. (Alden, col. 8, lines 31-56.) Thus, Alden does not teach or suggest an intermediate server "decrypting encrypted information," as recited in claim 56.

New Claims

Applicants have added new claims 61-81 to more fully claim their invention. Independent claim 66 recites a third intermediate computer that receives data from the first computer through the first firewall via a network connection initiated by the first computer, determines that the data received from the first computer is intended to be delivered to a second computer, and transmits the data to the second computer via a receive channel. Independent claim 74 recites a second computer in a communication network that receives data transmitted by a first computer through a first firewall via a network connection initiated by the first computer to a third intermediate computer, and then transmitted by the third intermediate computer to the second computer via a receive channel. Thus, for similar reasons discussed above regarding claims 55 and 57, independent claims 66 and 74 are allowable over the cited references. Claims 61-65, 67-73, and 75-81 depend respectively from claims 55, 66, and 74, and are allowable for at least the same reasons, as well as based on the additional features recited therein.

For example, claims 61-62, 71, and 79 recite wherein the intermediate server decrypts encrypted header information. Alden discusses general techniques for encryption, but neither Alden nor Erickson describes encrypting message headers, or decrypting header information at an intermediate server. Accordingly, Applicants submit that claims 61-62, 71, and 79 are allowable for at least this additional reason.

As another example, claims 63, 72, and 80 recite wherein communications between the intermediate computer and both of the endpoint computers is initiated by the endpoint computers. As discussed above, neither Alden nor Erickson describe any technique in which both of the communication endpoints initiate communication with an intermediate server. Thus, claims 63, 72, and 80 are allowable for at least this additional reason.

As yet another example, claims 64, 73, and 81 recite "wherein the first firewall and the

second firewall are configured not to allow incoming network messages, unless the incoming network messages are responsive to network messages initiated by a computer inside the firewall." As discussed above, Erickson only applies to communication between a client and server through a single firewall. In contrast, Alden describes communication across multiple firewalls, but only discloses techniques in which the firewalls must be programmed to pass packets received over transport layer connection into the private network on the other side of the firewall. (Alden, col. 6, lines 37-39.) Thus, neither Erickson nor Alden teaches or suggests communication across multiple firewalls "wherein the first firewall and the second firewall are configured not to allow incoming network messages, unless the incoming network messages are responsive to network messages initiated by a computer inside the firewall," as recited in claims 64, 73, and 81. Accordingly, claims 64, 73, and 81 are allowable for at least this additional reason.

Conclusion

Based on the foregoing, Applicants respectfully submit that the application is in condition for allowance and a Notice to that effect is earnestly solicited. Should the Examiner believe that anything further is desirable in order to place the application in even better form for allowance, the Examiner is respectfully urged to contact Applicants' undersigned representative at the below-listed number.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated this 5 day of June, 2007 By: 

Bradley C. Wright
Registration No. 38,061

1100 13th Street, N.W.
Washington, D.C. 20005
Tel: (202) 824-3160
Fax: (202) 824-3001